UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/321,977	05/28/1999	JOHN WANKMUELLER	AP32087-0704	7342

21003 7590 09/29/2004

BAKER & BOTTS
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/321,977	WANKMUELLER, JOHN	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 15-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,15-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-8 and 15-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1,2,6,7,15-18,21-29, and 31-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Bernstein, U.S. Patent 5,915,023.

As per claim 1, it is disclosed by Bernstein of a method for securely transmitting transaction data over a network having a public component wherein the transaction includes account PIN data and non-PIN data (col. 2, lines 38-50,60-63). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col. 12, lines 39-44). A second encryption operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13). It is interpreted that the examiner that since different

encryption operations are used to encrypt the PIN and non-PIN data, they are cryptographically isolated from one another. The cryptographically isolated PIN data and non-PIN data is then sent over the network (col. 8, lines 8-13,55-62).

As per claim 2, it is taught by Bernstein that the first encryption operation used public key, or asymmetrical, encryption process and the second encryption operation uses DES, or symmetric encryption (col. 1, lines 55-57, col. 8, lines 1-13, and col. 12, lines 42-44).

As per claim 6, Bernstein discloses of a method for decoding encrypted transaction data that includes account PIN data input by a user and non-PIN data that is received from a remote location across a network having a public location (col. 2, lines 38-50,60-63 and col. 8, lines 1-3,8-9). A first decryption operation is performed to decode the transaction (non-PIN) data (col. 1, lines 57-60 and col. 8, lines 1-3,8-13). A second decryption operation is performed to decode the PIN data and is different from the first decryption operation (col. 1, lines 55-57, col. 8, lines 1-3,8-9,50-62, and col. 12, lines 39-44).

As per claim 7, it is taught by Bernstein that the first decryption operation used public key, or asymmetrical, decryption process and the second decryption operation uses DES, or symmetric decryption (col. 1, lines 55-57, col. 8, lines 1-13, col. 8, lines 1-3,8-9, and col. 12, lines 42-44).

As per claim 15, Bernstein discloses of a method of transporting PIN data input by a user and non-PIN data in a secure electronic transfer (col. 2, lines 38-50,60-63). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col. 12, lines 39-44). A second encryption

operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13). The encrypted PIN and transaction (non-PIN) data are transmitted over a data network to an authentication requestor at a remote location and the authentication requestor only has means to decrypt the transaction (non-PIN) data wherein an authorizing agent decrypts and verifies the PIN (col. 7, lines 57-64 and col. 8, lines 8-13,55-62). A notification is transmitted over the data network from the authorizing agent to the authentication requestor listing the verification status of the PIN (col. 7, lines 57-64 and col. 8, line 55 through col. 9, line 12).

As per claim 16, it is taught by Bernstein that the first encryption operation used public key, or asymmetrical, encryption process and the second encryption operation uses DES, or symmetric encryption (col. 1, lines 55-57, col. 8, lines 1-13, and col. 12, lines 42-44).

As per claim 17, it is taught by Bernstein that the first encryption operation used public key, or asymmetrical, encryption process and the second encryption operation uses DES, or symmetric encryption (col. 1, lines 55-57, col. 8, lines 1-13, and col. 12, lines 42-44).

As per claim 18, Bernstein discloses of asymmetrical encryption is performed using a public key provided to an account holder by the authorizing agent and the decryption is performed by the authorizing agent using a private key associated with the public key (col. 7, lines 57-64, col. 8, line 55 through col. 9, line 12, and col. 12, lines 39-44).

As per claim 21, Bernstein teaches of a terminal (means) for encoding transaction data including account PIN data input by a user and non-PIN data (col. 2, lines 38-50,60-63). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col. 12, lines 39-44). A second encryption operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13). It is interpreted that the examiner that since different encryption operations are used to encrypt the PIN and non-PIN data, they are cryptographically isolated from one another. The cryptographically isolated PIN data and non-PIN data is then sent over the network (col. 8, lines 8-13,55-62).

As per claim 22, it is taught by Bernstein that the first encryption operation used public key, or asymmetrical, encryption process and the second encryption operation uses DES, or symmetric encryption (col. 1, lines 55-57, col. 8, lines 1-13, and col. 12, lines 42-44).

As per claim 23, Bernstein teaches of a card reader for acquiring the transaction data from a payment instrument (col. 9, lines 48-62).

As per claim 24, Bernstein discloses of a system for decoding encrypted transaction data that includes account PIN data input by a user and non-PIN data that is received from a remote location across a network having a public location (col. 2, lines 38-50,60-63 and col. 8, lines 1-3,8-9). A first decryption operation is performed to decode the transaction (non-PIN) data (col. 1, lines 57-60 and col. 8, lines 1-3,8-13). A second decryption operation is performed to decode the PIN

data and is different from the first decryption operation (col. 1, lines 55-57, col. 8, lines 1-3,8-9,50-62, and col. 12, lines 39-44).

As per claim 25, it is taught by Bernstein that the first decryption operation used public key, or asymmetrical, decryption process and the second decryption operation uses DES, or symmetric decryption (col. 1, lines 55-57, col. 8, lines 1-13, col. 8, lines 1-3,8-9, and col. 12, lines 42-44).

As per claim 26, Bernstein discloses of an apparatus (means) for transporting PIN data input by a user and non-PIN data in a secure electronic transfer (col. 2, lines 38-50,60-63). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col. 12, lines 39-44). A second encryption operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13). The encrypted PIN and transaction (non-PIN) data are transmitted over a data network to an authentication requestor at a remote location and the authentication requestor only has means to decrypt the transaction (non-PIN) data wherein an authorizing agent decrypts and verifies the PIN (col. 7, lines 57-64 and col. 8, lines 8-13,55-62). A notification is transmitted over the data network from the authorizing agent to the authentication requestor listing the verification status of the PIN (col. 7, lines 57-64 and col. 8, line 55 through col. 9, line 12).

As per claims 27 and 28, it is taught by Bernstein that the first encryption operation used public key, or asymmetrical, encryption process (col. 1, lines 55-57, col. 8, lines 1-13, and col. 12, lines 42-44). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col.

12, lines 39-44). A second encryption operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13).

As per claim 29, Bernstein discloses of a first encryption means that is performed using a public key provided to an account holder by the authorizing agent and the decryption is performed by the authorizing agent using a private key associated with the public key (col. 7, lines 57-64, col. 8, line 55 through col. 9, line 12, and col. 12, lines 39-44).

As per claim 31, Bernstein teaches of a card reader for acquiring the transaction data from a payment instrument that includes the PIN data and non-PIN data (col. 1, lines 55-60 and col. 9, lines 48-62).

As per claim 32, it is disclosed by Bernstein of an encrypted PIN and transaction (non-PIN) data are transmitted over a data network to an authentication requestor at a remote location and the authentication requestor only has means to decrypt the transaction (non-PIN) data wherein an authorizing agent decrypts and verifies the PIN (col. 7, lines 57-64 and col. 8, lines 8-13,55-62).

As per claim 33, Bernstein discloses of transmitting the encrypted PIN data to another remote location prior to performing the second decryption operation (col. 8, line 55 through col. 9, line 12).

As per claim 34, Bernstein teaches of decoding encrypted transaction data that includes an encrypted account PIN data encrypted by a first encryption operation as well as encrypted transaction (non-PIN) data encrypted with a second, different encryption operation. Transaction data is received from a

remote location over a network having a public component (col. 1, lines 55-60, lines 38-50,60-63, and col. 8, lines 1-3,8-13). A first decryption operation is performed to decode the encrypted transaction (non-PIN) data and transmitting the encrypted PIN to another remote location (col. 7, lines 57-64 and col. 8, lines 8-13,55-62).

As per claim 35, it is disclosed by Bernstein of performing a second decryption operation at the other remote location to decode the encrypted PIN data, wherein the second decryption operation is different from the first decryption operation (col. 1, lines 55-60, col. 7, lines 57-64, and col. 8, lines 8-13,55-62).

As per claim 36, Bernstein discloses that the remote location receiving the transaction data does not have the capability to decode the encrypted PIN (col. 8, lines 8-13,55-62).

As per claim 37, it is taught by Bernstein that the first decryption operation uses a symmetrical, DES, decryption process and the second decryption operation uses an asymmetrical, or public key, decryption process (col. 1, lines 55-57, col. 8, lines 1-13, col. 8, lines 1-3,8-9, and col. 12, lines 42-44).

As per claims 38 and 39, Bernstein discloses of a method of transporting PIN data input by a user and non-PIN data in a secure electronic transfer (col. 2, lines 38-50,60-63). A first encryption operation is performed only on the PIN data (col. 1, lines 55-57, col. 8, lines 50-62, and col. 12, lines 39-44). A second encryption operation is performed on the transaction number (non-PIN) data (col. 1, lines 57-60, col. 8, lines 8-13). The encrypted PIN and transaction (non-PIN)

data are transmitted over a data network to an authentication requestor at a remote location and the authentication requestor only has means to decrypt the transaction (non-PIN) data wherein an authorizing agent decrypts and verifies the PIN (col. 7, lines 57-64 and col. 8, lines 8-13,55-62). A notification is transmitted over the data network from the authorizing agent to the authentication requestor listing the verification status of the PIN (col. 7, lines 57-64 and col. 8, line 55 through col. 9, line 12).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3,4, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernstein, U.S. Patent 5,915,023 in view of McKinsey.

As per claims 3 and 19, Bernstein discloses of separately encrypting PIN data and non-PIN data. Bernstein further discloses of the use of symmetric encryption that uses DES (secret key) to encrypt the transaction (non-PIN) data (col. 8, lines 1-13). The teachings of Bernstein are silent in disclosing that a third encryption operation is performed on the secret encryption key. McKinsey discloses of encrypting a symmetric key with a public key (pg 3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to

have been motivated to re-encrypt a key so it is protected. McKinsey recites motivation of encrypting a symmetric key by disclosing that the intent is to protect sensitive data from unauthorized usage (pg 1). Since the teachings of Bernstein are directed towards protecting financial information, it is obvious that McKinsey offers further protection by encrypting the session keys.

As per claim 4, Bernstein discloses of separately encrypting PIN data and non-PIN data. The teachings of Bernstein are silent in disclosing of an encrypted envelope that includes PIN and non-PIN data. It is disclosed by McKinsey of a Cryptolope container (encrypted envelope) which includes content (non-PIN data) and control information (PIN data) to be transferred together and the content are encrypted with a symmetric key that is encrypted with a public key (pg 2 & 3). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a means for securely protecting data. McKinsey discloses motivation for the use of Cryptolope containers (encrypted envelopes) by reciting that it allows for both content (non-PIN data) and control information (PIN data) to be transferred together (pg 2). It is obvious that the teachings of Bernstein would have benefited from the disclosure of McKinsey as a means of transferring PIN and non-PIN together in a secure manner by means of a Cryptolope container (encrypted container) to allow for the protection of proprietary information from an illicit user.

6. Claims 5,8,20, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernstein, U.S. Patent 5,915,023.

The teachings of Bernstein are silent in disclosing of calculating a digest by applying a one-way mathematical process and to append the digest for future verification. The examiner hereby takes official notice that the use of hashing to be appended to a file and later recomputing the hash to see if the information has not be altered based on the hash values matching is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use hashing for data verification purposes. Hashing is notoriously well known as a one-way mathematical process which converts data to a specific value and when recomputing the data using the same hashing function should produce the same hash value that indicates that the data has maintained its integrity. Otherwise, if the recomputed hash values do not match with the original has value, then it is determined that the data has been altered. It is obvious that the teachings of Bernstein would have benefited from the use of hashing as a means of maintaining the integrity of the proprietary information since are directed towards a secure processing system.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Please see attached PTO-892

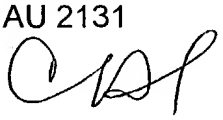
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone

number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131



9/21/04

CR

September 21, 2004